CLAIMS

1. A method of creating a certificate to certify a key, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate,

characterized by the following steps:

a) Specification of a request for certification of one of the several keys by a certification body for a user.

b) If in step a) only one key is to be certified, and no basic certificate is yet available for the user, creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body.

c) Addition of an identifying characteristic to the basic certificate.

d) Generation of a digital signature for the basic certificate.

e) Addition of the digital signature to the basic certificate.

f) Generation of a key pair.

g) Creation of a supplementary certificate for the basic certificate with a key as set out in step f), the identifying characteristic as set out in step c) and additional data fields not registered by the basic certificate.

h) Generation of a digital signature for the supplementary certificate.

i) Addition of the digital signature to the supplementary certificate.

2. The method in accordance with Claim 1, characterized in that the basic certificate comprises the following data elements:
- Name of certification body
- User ID of certification body
- Name of user
- User ID of user
- Identifying characteristic of the basic certificate

3. The method in accordance with Claim 1, characterized in that the supplementary certificate comprises the following data elements:
- Signature algorithm
- Key
- Serial number of key
- Validity period of the certificate
- Extensions
- Identifying characteristic of the basic certificate

4. The method in accordance with Claim 1, characterized in that if step a) reveals that more than one key with the same validity period is to be certified at one time, instead of steps b) - i) the following steps are executed:

aa) Generation of several key pairs.

bb) Generation of a certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), omitting the redundant data elements.

cc) Generation of a digital signature for the certificate.

dd) Addition of the digital signature to the certificate.

5. The method in accordance with Claim 4, characterized in that the certificate contains the following data elements:
- Name of certification body
- User ID of certification body
- Name of user
- User ID of user
- Type/version of the certificate
- Number and types of keys
- Key
- Validity
- Serial number
- Extensions

6. The method in accordance with Claim 1 characterized in that, if only one key is to be certified in step a) and a basic certificate already exists, instead of steps b) - i) the following steps are executed:

aa) Definition of the basic certificate and reading of the identifying characteristics of the basic certificate.

bb) Generation of a key pair.

cc) Creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate in step bb).

dd) Insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate.

ee) Generation of a digital signature for the supplementary certificate.

ff) Addition of the digital signature to the supplementary certificate.

7. The method in accordance with Claim 6, characterized in that the supplementary certificate contains the following data elements:
   - Signature algorithm
   - Key
   - Serial number of key
   - Validity period of the certificate
   - Extensions
   - Identifying characteristic of the basic certificate

8. The method for creating a certificate for simultaneous certification of several keys with the same validity period, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate, characterized by the following steps:

   aa) Generation of several key pairs.

   bb) Generation of a joint certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), omitting the redundant data elements.

   cc) Generation of a digital signature for the group certificate.

   dd) Addition of the digital signature to the group certificate.

9. The method in accordance with Claim 8, characterized in that the group certificate contains the following data elements:
   - Name of certification body
   - User ID of certification body
   - Name of user
   - User ID of user
   - Type/version of the certificate
   - Number and types of keys
   - Key
   - Validity
   - Serial number
   - Extensions

10. A method for creating a certificate for certification of a new key for a user, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate, wherein a basic certificate for the user already exists and the basic certificate comprises data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body, characterized by the following steps:

    aa) Definition of the basic certificate for the user and reading of the identifying characteristics of the basic certificate.

    bb) Generation of a key pair.

cc) Creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate in step bb).

dd) Insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate.

ee) Generation of a digital signature for the supplementary certificate.

ff) Addition of the digital signature to the supplementary certificate.

11. The method in accordance with Claim 10, characterized in that the supplementary certificate contains the following data elements:
- Signature algorithm
- Key
- Serial number of key
- Validity period of the certificate
- Extensions
- Identifying characteristic of the basic certificate

12. The method in accordance with Claim 8, characterized in that the key is a public key.

13. The method in accordance with Claim 1, characterized in that the basic certificate and the supplementary certificate are stored in the non-volatile memory of a chipcard.

14. The method in accordance with Claim 4, characterized in that the certificate (group certificate) is stored in the non-volatile memory of a chipcard.

15. The method for reading certificates created in accordance with Claim 1, characterized by the following steps:

a) Check of the storage medium for presence of basic certificates.

b) If present, identification of the necessary supplementary certificate.

c) Read-in of the supplementary certificate to the RAM of a system.

d) Definition of the identification number of the basic certificate from the supplementary certificate.

e) Read-in of the basic certificate to the RAM.

16. The method in accordance with Claim 15, characterized in that, if no basic certificate could be identified in step a), instead of steps b) - e) the following steps are executed:

f) Check of the storage medium for presence of group certificates.

g) Read-in of the necessary group certificates to the RAM.

17. The method for reading of certificates created in accordance with Claim 10, characterized by the following steps:

    a) Check of the storage medium for presence of group certificates.

    b) Read-in of the necessary group certificate to the RAM.

18. The method in accordance with Claim 17, characterized in that the storage medium is a non-volatile memory of the chipcard.

19. A computer program product on a computer usable medium for creating a certificate to certify a key, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer to the certificate), the user of the certificate and the key certified by the certificate, said computer program product comprising:

    a) software for specification of a request for certification of one of the several keys by a certification body for a user;

    b) software for creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body when only one key is to be certified, and no basic certificate is yet available for the user;

c) software for the addition of an identifying characteristic to the basic certificate;

d) software for the generation of a digital signature for the basic certificate;

e) software for the addition of the digital signature to the basic certificate;

f) software for generation of a key pair;

g) software for creation of a supplementary certificate for the basic certificate with a key as set out in f), the identifying characteristic as set out in c) and additional data fields not registered by the basic certificate;

h) software for generation of a digital signature for the supplementary certificate; and

i) software for addition of the digital signature to the supplementary certificate.

20. The computer program product in accordance with Claim 19, characerized in that the basic certificate comprises the following data elements:

- Name of certification body
- User ID of certification body
- Name of user
- User ID of user
- Identifying characteristic of the basic certificate.

21. The computer program product in accordance with Claim 19, characterized in that the supplementary certificate comprises the following data elements:

- Signature algorithm
- Key
- Serial number of key
- Validity period of the certificate
- Extensions
- Identifying characteristic of the basic certificate.

22. The computer program product in accordance with Claim 19, characterized in that if more than one key with the same validity period is to be certified at one time, the following software replaces the software of b) to i);

aa) software for generation of several key pairs;

bb) software for generation of a certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), omitting the redundant data elements;

cc) software for generation of a digital signature for the certificate; and

dd) software for addition of the digital signature to the certificate.

23. The computer program product software in accordance with Claim 22, characterized in that the certificate contains the following data elements:

- Name of certification body
- User ID of certification body
- Name of user
- User ID of user
- Type/version of the certificate
- Number and types of keys
- Key
- Validity
- Serial Number
- Extensions.

24. The computer program product in accordance with Claim 19, characterized in that, if only one key is to be certified and a basic certificate already exists, the following software replaces the software of b) to i):

aa) software code definition of the basic certificate and reading of the identifying characteristics of the basic certificate;

bb) software code for generation of a key pair;

cc) software code for creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate by step bb);

dd) software code insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate;

ee) software code generation of a digital signature for the supplementary certificate; and

ff) software code addition of the digital signature to the supplementary certificate.

25. The computer program product in accordance with Claim 24, characterized in that the supplementary certificate contains the following data elements:

- Signature algorithm
- Key
- Serial number of key
- Validity period of the certificate
- Extensions
- Identifying characteristic of the basic certificate.